REMARKS

This paper is being filed as a response to the Final Office Action of September 26, 2007. Reconsideration is respectfully requested in view of these clarifying remarks.

Rejections under 35 USC § 103(a)

Claims 1, 3, 4, 9-11, 25, 27, 29 and 30 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Rowland (US Publication No. 2002/0129264). This rejection is respectfully traversed. Applicant respectfully requests reconsideration of these rejections in light of the arguments contained herein.

Claim 1 defines a kernel module signature verification system for verifying said kernel module signature information of each of said plurality of kernel modules as said plurality of kernel modules are loaded into said kernel (emphasis added). The Office has relied on the following excerpt from Rowland to suggest the Applicant's claim:

> "[0149] Loadable Kernel Module Agent 1306--This agent looks for known or unknown loadable kernel modules (LKMs) for UNIX® compatible systems. Modified LKMs are a common method used by attackers to conceal activity on compromised systems. This agent looks for the following: unauthorized LKMs loaded; known suspicious LKMs loaded; unknown suspicious LKMs loaded; intercepting system calls; employing protective anti-probe or stealth techniques; accessing or hooking normally restricted data areas in memory or on disk; and other suspicious activity." (Parg. [0149], emphasis added)

The Examiner has asserted that "Kernel Agent Module 1306 ... is an agent looking for loadable kernels and verifies their validity" (emphasis added). Applicant respectfully disagrees. Rowland teaches that the Loadable Kernel Module Agent looks for kernel modules, but there is no suggestion that the Loadable Kernel Module Agent verifies the kernel modules. Furthermore, the Loadable Kernel Module Agent looks for LKMs that are already loaded, that is quite different from verifying said kernel module signature information when said plurality of kernel modules are loaded. Verifying a kernel module before being loaded protects the system from malicious kernel modules being loaded, but Rowland only teaches how to look for modules that have already been loaded in compromised systems in order to take corrective action. Therefore, Rowland does not suggest verifying said kernel module signature information of each of said plurality of kernel modules as said plurality of kernel modules are loaded, as claimed.

Still yet, the Office has used the additional excerpt below to show how Rowland teaches the use of "signatures to identify intrusions such as suspect loadable kernel modules."

> "[0148] Known Intrusion Agent 1305 This agent is designed with signatures specifically to look for and alarm on signs of known intrusion. This agent is designed to randomly roam the network and detect this activity before it becomes widespread. Upon detection it notifies the central server that can then dispatch Intrusion Control Agents, Forensic Evidence Agents, or other MAC Agents to assess and respond to the incursion. The signatures that this agent rely upon are varied depending on the type of attack, but they can include: known Trojan horse detection; common backdoors; common binary alterations; suspicious directories which are known hiding places for attackers; suspicious files, for example files with known suspicious filenames indicating a break-in attempt or success; tampered system critical files; suspicious loadable kernel modules; suspicious running operating system modifications; suspicious usernames; known suspicious usernames; usernames that were not present on the system last time it was scanned; usernames that are not authorized to be present on the system regardless of last time scanned; altered or missing log files; altered or missing accounting records; and other suspicious activity as specified in the accompanying database with the agent." (Paragraph [0148] - emphasis added)

Applicant respectfully disagrees. The Office has misinterpreted the meaning of the term 'signature' as used by Applicant. The Office has used the website webopedia.com to forward an industry definition of a computing term, so the Applicant will refer to the same website to describe the different meanings of the word 'signature.' Applicant refers to signature as digital signature that webopedia defines as "[a] digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be. Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes" (emphasis added). On the other hand, in Paragraph [0148] Rowland refers to signature as something that leaves a trail or mark, for example a "virus [Trojan horse] signature," that webopedia defines as "[a] unique string of bits, or the binary pattern, of a virus."

Rowland teaches how to look for signatures left by malicious code or activities, but it's not referring to signatures where "information is generated via a public key and a private key," as claimed. Rowland is referring to a different type of signatures, and the Office's rejection is therefore moot.

Claim 1 further describes wherein said kernel module signature information is generated via a public key and a private key compilation in said kernel module. The Office has asserted that the "use of public and private keys to create signature verification protocol is well-known in the art." Applicant respectfully disagrees. The use of kernel module signature information is not well known in the art, and definitively not suggested by Rowland, as discussed hereinabove. Applicant respectfully traverses. Note excerpt from MPEP below.

"If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

The Office has failed to provide a specific showing of the subject matter in ALL of the claims. Applicants formally request a specific showing of the subject matter in all of the claims in any future action.

Claim 1 further defines a kernel module signature verification system that includes ... a kernel cryptographic framework for verifying said kernel module signature information. The Office has relied on the following paragraph to suggest Applicant's claim:

> "[0132] 1. [One of the primary responsibilities of the Agent Handler is] To ensure the MAC modules carry appropriate credentials and are authenticated and cryptographically signed by a trusted introducer (network administrator, operator, client system, etc.)." (Paragraph [0132])

Rowland also teaches that "Mobile Autonomous Code (MAC Agents) are independently distributed pieces of code that operate within a special execution environment within the client and server system", and that "MAC Agents are capable of moving between systems independent of the actual client, and that "[t]he MAC operate within a separate execution environment from the rest of the system that can be open or restricted depending on configuration" (Paragraph. [0137]). On the other hand, Applicant claims kernel modules that are closely tied to the kernel inside an operating system. Webopedia defines the term 'kernel' as:

> "The central module of an operating system. It is the part of the operating system that loads first, and it remains in main memory. Because it stays in memory, it is important for the kernel to be as small as possible while still providing all the essential services required by other parts of the operating system and applications. Typically, the kernel is responsible for memory management, process and task management, and disk management."

However, a MAC agent that operates within a separate execution environment from the rest of the system would hardly qualify as a kernel module because a kernel module is tightly related with the operation of the system, managing items like memory, processes, tasks and disks. Furthermore, a MAC agent is capable of moving between systems independent from the rest of the system, while a kernel is tightly coupled with the system in which it operates. Therefore, a MAC agent does not suggest a kernel module and thus, it can not suggest a kernel cryptographic framework, as claimed by Applicant.

Additionally, Claim 1 describes a kernel cryptographic framework daemon for performing verification lookup operations of signature information provided to said kernel cryptographic framework. The Office once again has relied on a module, Suspicious File Agent, "designed to look for known or user-specified banned files," to suggest the aforementioned claim. As discussed hereinabove, verifying a module is different from looking for a malicious file already in the system, and the Office's rejection is also improper.

Office Response to Arguments

The Office has asserted that the Applicant does not explain what is the specific way and form of the claimed use of encryption, and how this specific way distinguishes the invention from the prior art.

Applicant has described supra how Rowland does not refer to kernel modules, but code that travels in the network and can be run by servers or clients. Applicant has also asserted that the prior art does not teach using private key encryption for kernel modules. Applicant has provided many examples on how the use of encryption in the claims is new and different from prior art, as noted in the above arguments. The Applicant has traversed Examiner's rejection and has requested that the "examiner should cite a reference in support of his or her position" (see MPEP 2144.03).

The Office has asserted that "it would have been obvious to the one skilled in the art to use public and private keys to create the signature information contained in the cited prior art's kernel modules." The Office has not articulated reasoning with rational underpinning to support the conclusion of obviousness. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit, *In re KSR International*

Co. v. Teleflex Inc. (KSR), 550 U.S. _, 82 USPQ2d 1385 (2007). The Court in KSR quoted *In re Kahn*, which stated that ''[R]ejections on obviousness cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.'' The Office's has not provided a justification for the suggestion of obviousness. Thus, the Office has merely put forth conclusory statements and not provided articulated reasoning to support the legal conclusion of obviousness.

Furthermore, in the Response to Arguments for the Office Action dated September 26, 2007, the Examiner has pointed to Paragraph [0148], excerpted above, from Rowland to suggest that "the agents verify the signatures of suspicious loadable kernel modules [and that] the kernel modules are to be loaded onto the system." Applicant respectfully disagrees. Rowland teaches that the Known Intrusion Agent is designed with signatures specifically to look for and alarm on signs of known intrusion. The Known Intrusion Agent acts after a system has been compromised, and does not act to verify kernel modules before they are loaded. In fact, the Known Intrusion Agent is looking for 'signatures' of malicious activity, and not using the 'digital signatures' claimed by Applicant, as discussed above.

In view of the foregoing, the Office is requested to withdraw the rejection of Claim 1 under §103. Independent Claim 25 is submitted to be patentable for at least the same reasons Claim 1 is believed to be patentable. The dependent claims are submitted to be patentable for at least the same reasons the independent claims are believed to be patentable. The Applicants therefore respectfully request reconsideration and allowance of the pending claims. A Notice of Allowance is respectfully requested.

If the Examiner has any questions concerning the present amendment, the Examiner is kindly requested to contact the undersigned at (408) 774-6920. If any other fees are due in connection with filing this amendment, the Commissioner is also authorized to charge Deposit Account No. 50-0805 (Order No. SUNMP459). A duplicate copy of the transmittal is enclosed for this purpose.

Respectfully submitted,
MARTINE PENILLA & GENCARELLA, LLP

/Jose M. Nunez/

Jose M. Nunez
Reg. No. 59,979

710 Lakeway Drive, Suite 200
Sunnyvale, CA 94085
Telephone: (408) 749-6900
Facsimile: (408) 749-6901